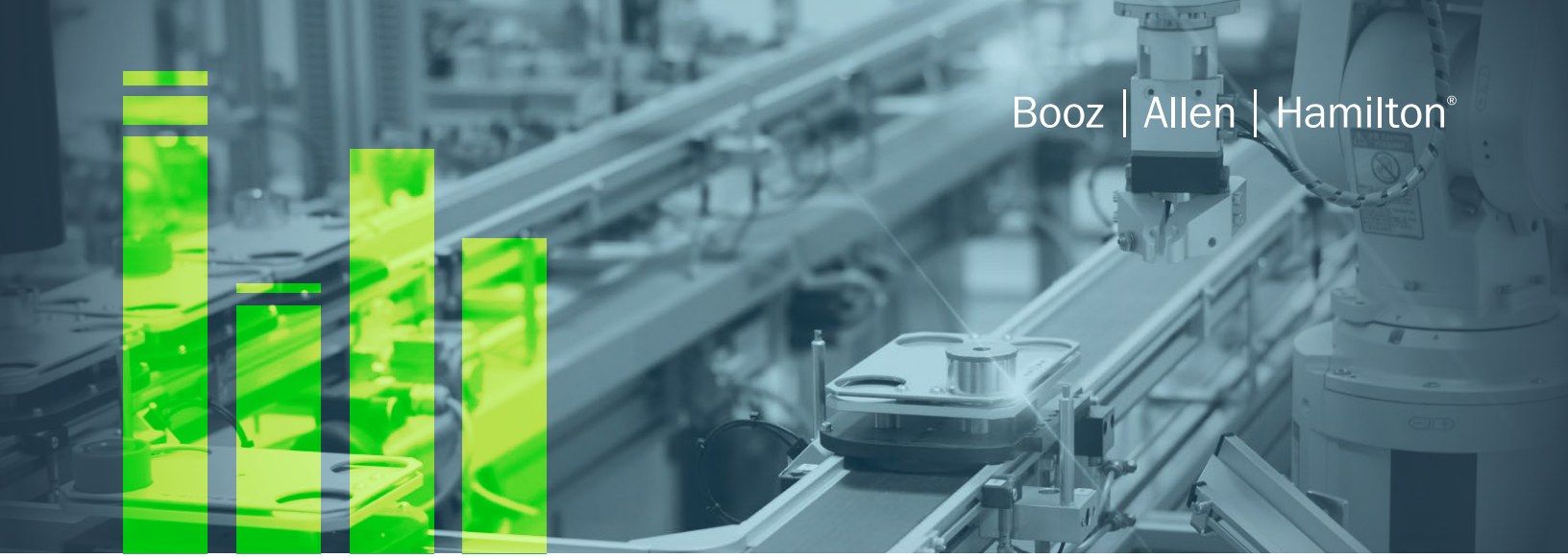
Booz | Allen | Hamilton®

2021 TECHNOLOGY SPOTLIGHT

UBIQUITOUS THREATS: CYBER AND IOT/OT

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER



The proliferation of the Internet of Things (IoT) for consumers and enterprises and the networking of Operational Technology (OT) introduce new opportunities to minimize vulnerabilities and enhance security. However, for all its benefits, IoT/OT's "ubiquitous compute" will also mean ubiquitous threats.

Society's continued arc towards interconnectedness is leading to increased efficiency, productivity, and convenience. Connected homes, vehicles, phones, appliances, devices, platforms, and cities provide benefits to consumers, enterprises, and governments alike, but this increased connectedness of IoT environments has also produced a corresponding spike in cybersecurity vulnerabilities, malware attacks, and data protection needs. Today, cybersecurity news often focuses specifically on Information Technology (IT) systems because of the risks in how data can be exposed and stolen during attacks.

More and more, however, Operational Technology (OT) connected to IoT environments is becoming an area recognized as critical for organizations to address distinctly from simply copying-and-pasting IT cybersecurity best practices. While IT is about data, OT is about processes and making things happen via control systems. Thus, when OT systems and devices are connected in IoT environments, cybersecurity for OT requires not just the protection of IP and data, but also the protection of the availability, integrity, reliability, productivity, and safety of the physical devices themselves, which in turn may be critical to ensuring human safety and preventing material loss.

Additionally, given the increasing frequency of IoT devices being deployed throughout enterprise and industrial networks today, IoT/OT devices are being more commonly seen as a potential attack vector, especially where their "soft target" status may be used as the launching point for a larger impact attack. To respond to this changing threat landscape, organizations must develop clear processes organized around third-party risk management, asset identification, automated processes, and monitoring to allow more visibility into the current security control of their vendors and shed light on vulnerabilities in the supply chain.

WHAT IS THE ROLE OF CYBERSECURITY IN IOT/OT ENVIRONMENTS?

Traditional cybersecurity efforts focus on securing data and intellectual property, but cybersecurity for IoT/OT requires that and more: protection of physical devices, protection of every component and system that devices interact with, and protection of the various layers and methods of communication to facilitate those interactions and the processes they support. The proliferation of interconnected devices in the IoT ecosystem has produced a corresponding increase in IoT-based malware attempts as organizations struggle to provide adequate protection measures. Since 2016, enterprises have seen a +831% increase in data that need to be managed,[1] but experience a plethora of challenges related to securing this data.

Within the context of OT, this incredible growth of IoT devices means that the attack surface of IoT/OT environments has grown significantly in recent years. To have visibility of this expanded attack surface, organizations must first understand the risks associated with third-party vendors and suppliers. Outsourcing and segmentation have reduced the costs of commercial-off-the-shelf (COTS) devices, while also creating security and trust issues within the supply chain. Many third-party vendors use IoT/OT devices that run off simplified or legacy operating systems and software frameworks that do not support the same level of security protections or network visibility as traditional IT systems. Because of this, these devices have the potential to increase a supply chain's attack surface and become a weak link in the cybersecurity chain.

The need for cybersecurity in IoT/OT environments is clear: the lack thereof puts enterprise security, the supply chain, and individual privacy at risk, with massive consequences ranging from financial and manufacturing damages to national security harm to significant risks to life and safety. As IoT management needs become more pronounced, cybersecurity will play an even more prominent role in the IoT/OT ecosystem, touching every layer of the tech stack: device security, network security, cloud security, and secure lifecycle management. Truly effective OT cybersecurity will need to provide end-to-end protection of each of these layers.

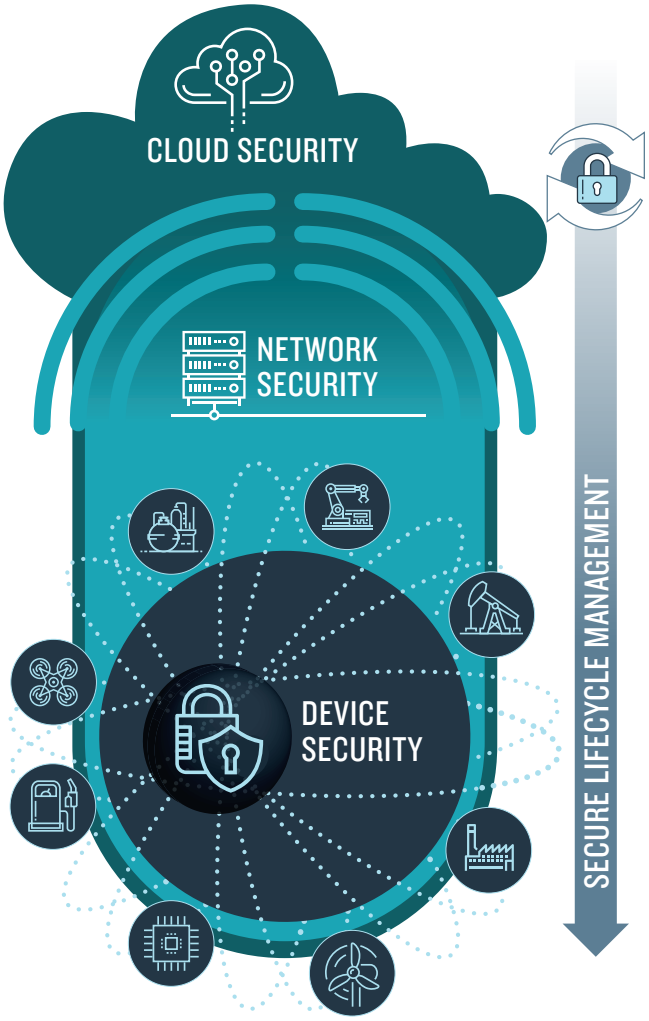


Figure 1: Cybersecurity & IoT/OT Layers

[1] "Dell Technologies Research: Cyber Attacks and Disruptive Events Are on the Rise, Affecting 82% of Organizations Surveyed," https://www.prnewswire.com/news-releases/dell-technologies-research-cyber-attacks-and-disruptive-events-are-on-the-rise-affecting-82-of-organizations-surveyed-301021374.html. *PR Newswire*.

A CLOSER LOOK: CYBERSECURITY & IOT/OT LANDSCAPE

Any technology ecosystem consists of, or can be broken down into, a set of core components. Over time, capabilities and offerings sprout up around these core components as they mature. To fully understand a technology, it is often easier to analyze the individual components. We identify the following core capabilities for the application of cybersecurity in the IoT/OT ecosystems:

Core Capabilities	What It Is	Purpose
CONTINUOUS MONITORING	The process and technology used to detect compliance and risk issues associated with an organization's financial and operational environment. The financial and operational environment consists of people, processes, and systems working together to support efficient and effective operations. Controls are put in place to address risks within these components.	Continuous monitoring helps organizations assess and understand their systems and processes in real-time. An organization using third-party service providers that have virtual access to IoT/OT systems must establish a certain level of trust and transparency. By building relationships with suppliers, organizations can work together to track risk factors such as ownership, manufacturing locations, supplier relationships, and available attack surface. Given their frequent lack of security robustness and overall interconnectedness, the chief concern is that new IoT environments become a soft target for an adversary and are used as the launching point for a larger impact attack.
THREAT INTELLIGENCE	The practice of collecting data, information, and knowledge that keep an organization informed about potential cybersecurity threats.	The risks of supply chain attacks are greater now than ever before. Threat intelligence can help organizations understand the risks associated with their portfolio of third-party vendors and suppliers. Organizations should be able to identify the most valuable assets that may be targets, such as intellectual property, proprietary information, and customer information. By understanding adversary motivations, an organization can determine which areas of the IoT/OT supply chain are most vulnerable and how to prioritize cybersecurity investments.
THREAT DETECTION	The practice of analyzing the entirety of a security ecosystem to identify any malicious activity that could compromise the network. If a threat is detected, then mitigation efforts must be enacted to properly neutralize the threat before it can exploit any present vulnerabilities.	Visibility of this expanded attack surface is the key to security—and the challenge. Without high confidence visibility into your supplier security levels and protocols, it is extremely difficult to understand whether inbound materials or systems have been compromised.
INCIDENT RESPONSE	An organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident, or security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.	Stopping attacks before they cause damage is the goal in any cybersecurity approach, but incidents are still possible as attackers evolve their tactics. Organizations should take the time to understand the extent of their existing IoT devices, their locations within the network, and their risk profile so that they can effectively respond to potential threats. By having set response procedures (prior to incidents) and a proactive understanding of current attack types, organizations can better identify attacks in the moment and address impacted devices and systems.

A LOOK AT THE CYBER IOT/OT MARKET

Given both the benefits and the necessity of cybersecurity measures for the IoT/OT ecosystem, the market is growing rapidly in terms of both deal count and investment. Over the past 5 years, the market has matured as venture capital (VC) firms double-down on market winners in their portfolios, directing funds to startups that are maturing and proving out their capabilities. Early stage deals (Seed and Series A) have gone from a high of 75% of total deals in 2016 to a low of 20% in 2020, while late stage deals (Series C, D, and E) have gone from a low of 9% in 2017 to a high of 40% in 2020.

These mirrored trends reveal a maturing market, which means there are many late-stage IoT security startups that are well-capitalized and growing fast. A maturing market also signals customer demand and proven success, again highlighting the increasing relevance and prominence of startups in this space. Some of 2020's large late-stage investments include SentinelOne ($200M Series E in February) and Axonius ($58M Series C in March). Chart 1 provides more insights below.

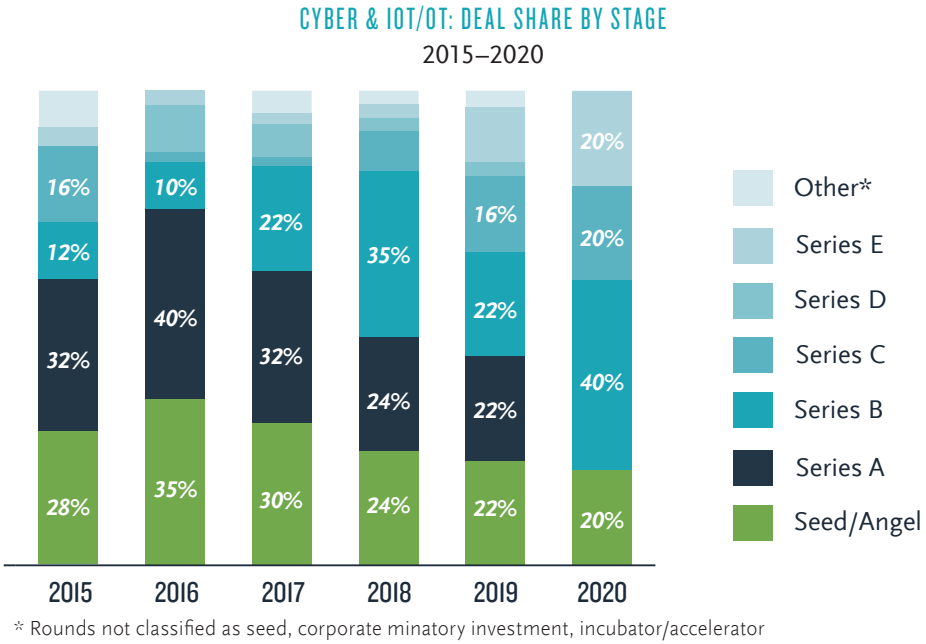


Chart 1: Cyber & IoT/OT Market by Stage.

Source: CB Insights and Booz Allen analysis.

An increase in acquisitions is likely, not only due to the natural maturing and proven success of startups' offerings, but also given the 67% reduction in available VC funding, for the intersection of cybersecurity and IoT from COVID-19. As the pandemic affects the global economy as well as the cyber IoT/OT market now and into the future, it is likely that startups will pivot to acquihire and acquisition opportunities given fluctuating VC funding. Recent IoT/OT security platform acquisitions in 2020 include CyGlass (acquired by UK-based cyber provider Nominet), Forescout (acquired by PE firms Advent and Crosspoint Capital), and most notably, CyberX (acquired by Microsoft).

SECURING THE IOT/OT ECOSYSTEM

TAKEAWAYS FOR YOUR ORGANIZATION

High-Impact Industries: Given the massive cyber incident risks that could occur in critical systems—from life support to water systems and supply chains—organizations need to advance their OT security capabilities beyond compliance and into an integrated enterprise approach. For example, America's at-risk networks in industries such as healthcare and energy/grid security, should explore the provisioning of network segmentation, visibility solutions, and endpoint protection. Within hospitals, imaging systems and patient monitoring devices both have known vulnerabilities—and both also happen to be integral parts of COVID patient care. And within the energy sector, the wind plan lifecycle involves many parties and effective cybersecurity practices are difficult to establish, maintain, and trace through the supply chain. Focus on increasing the practices around cyber threat, vulnerability, incident, and mitigation while limiting information sharing.

Partnerships: Not all IoT is built with the same level of security protections and each has the potential to introduce new risks. It's essential to understand what security controls each partner has in place, from encryption to access control procedures, to ensure awareness of possible exposure across the enterprise. On the security integration front, partnerships will be central for a comprehensive strategy. With a technical integrator, optimize channel partnership opportunities across each component layer of the cyber IoT/OT ecosystem to implement best-in-class capabilities for enhanced security with cutting-edge technology and innovative approaches.

Technical Investments: Consider OT passive monitoring tools, next-generation firewalls/network segmentation and OT threat detection along with sub-trends such as intent-based networking (IBN) that minimize human intervention and provide maximum network security. Later on, consider less pervasive technologies in the OT environments like software-defined networking options that are just starting to get talked about and allow for configuration as needed.

Workforce Transformation: As IT, IoT, and OT converge across industries and begin to be managed under common governance within organizations, employees will experience both the benefits and responsibilities of greater access to operational data across devices and networks. In utilizing a unified approach to IoT/OT, technology professionals will need strong cybersecurity support to understand how shared data can be used securely to meet organizational goals.

FOR MORE INFORMATION:

The content in this 2021 Technology Spotlight Series originates from Booz Allen's emerging technologies capabilities as part of our innovation agenda, and this spotlight on Cyber and IoT/OT was developed by Booz Allen's Technology Scouting team. For more in-depth security guidance, please visit **BoozAllen.com/cyber**.

About Emerging Technologies at Booz Allen

For over a century, Booz Allen has been at the forefront of technology and strategy. We provide strategic advisory services, design, build, and deploy solutions across sectors to a wide range of federal government organizations. We are the only management and technology consulting firm that has invested in an innovation network exclusively focused on scouting dual-use technologies for federal government missions. As a result, we successfully partner with the tech community to showcase a wide range of capabilities and deliver innovative solutions to our clients.

Our deep pool of technical talent, access to critical networks in innovation hubs, and experience performing tech scouting across technologies and sectors uniquely position Booz Allen to serve clients who seek to be at the cutting edge.

To learn more, visit BoozAllen.com (NYSE: BAH)